REMARKS

Claims 1-18 are pending in the current application. In an office action dated August 2, 2007 ("Office Action"), the Examiner rejected claims 1-18 under 35 U.S.C. §103(a) as being unpatentable over Schneck et al., U.S. Patent No. 6,865,426 ("Schneck") in view of Jones, U.S. Patent No. 5,412,730 ("Jones"). Applicant's representative respectfully traverses these rejections.

In a previous office action, the Examiner rejected the current claims as being anticipated by Arbaugh et al., U.S. Patent No. 6,185,678 ("Arbaugh"), even though, as Applicant's representative pointed out in a previously filed response, Arbaugh contained no teaching or suggestion of the second element of claim 1 "a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system." Thankfully, the Arbaugh reference has been dropped. However, in the current Office Action, the Examiner has again relied on references that do not teach, mention, or suggest the second element of claim 1, "a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system," and the second element of claim 9, "providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium local to the monitor computing device, and the other data-storage medium local to the remote computer system."

One embodiment of the data-storage media to which the second elements of claims 1 and 9 are directed is shown in Figure 6 of the current application. In the described embodiment, the data-storage media are CD-read/write devices. The CD-read/write devices and are shown positioned within a system (510 and 512) in Figure 5 of the current application.

The Examiner states, on page 3 of the Office Action, that "Jones teaches a pair of data-storage media each containing a sequence of encryption keys (see Jones figure 1 element 23 and 27)." Elements 23 and 27 of Figure 1 of Jones are pseudo-random number generators, and are clearly labeled as such. Those familiar with

electronics and computing well understand that a pseudo-random number generator is not a sequence of encryption keys, but is instead an electronic circuit or executable routine that generates pseudo-random numbers by one of many possible pseudo-random-number-generation algorithms. These pseudo-random-number-generation algorithms generally employ a seed number or value to initialize the circuit or routine, and then generate pseudo-random numbers one after another, when requested to do so. Indeed, Jones describes operation of the pseudo-random number generator (23 in Figure 1), beginning on line 34 of column 3, as follows:

> The advance signal produced by block counter 21 is supplied to the advance input of a pseudo-random number generator 23 which supplies a sequence of encryption key values to the key input of the encryptor 17. *The content of the key sequence is predetermined by the combination of (1) the internal makeup of the generator 23 and by (2) a supplied random number seed value which initializes the generator 23. The generator 23 responds to each advance signal from block counter 21 by changing its output to the next successive encryption key value.* (emphasis added)

A pseudo-random number generator is not a data-storage medium containing a sequence of encryption keys. Jones does not teach, mention, suggest, or even imply any kind of pair of data-storage media, each containing a sequence of encryption keys. Indeed, Jones' pseudo-random number generator supply an electronically encoded sequence of pseudo-random numbers, but do so one pseudo-random number at a time, and generate each pseudo-random number algorithmically, rather than employing a stored list of pseudo-random numbers. That is why they are called "pseudo-random number <u>*generators*</u>," and not "sequences of pseudo-random numbers," as those familiar with computer science well understand.

As the Examiner hopefully appreciates, even in an obviousness-type rejection in which references are combined, the combination of references must nonetheless teach or suggest all of the claim limitations, as explicitly stated in M.P.E.P. § 2142. Neither Jones nor Schneck teaches, mentions, or suggests a pair of data-storage media each containing a sequence of encryption keys.

While the second element of both independent claims is not taught or suggested by either cited reference, the 35 U.S.C. §103(a) rejections based on Schneck

and Jones are unjustified for additional reasons. For example, in the Office Action, the Examiner states: "With respect to claim 1, Schneck teaches a monitor that monitors the security state of a remote computer system, the monitor comprising: a computing device (see figure 1 element 106 Receive Host) and a communications medium interconnecting the computing device with the remote computer system (see figure 1 element 103 Send Host). Hopefully, the Examiner will appreciate that a reference to a block of a block diagram that has nothing to do with monitoring the security state of a remote computer system can hardly serve as justification for a rejection of either claim 1 or claim 9, or any claim dependent from either claim 1 or claim 9. Schneck does not teach, mention, or suggest anything at all concerned with monitoring the security state of a computer system. Instead, as clearly stated by Schneck in the abstract, Schneck "relates to a method for communicating and applying adaptive security to a data stream comprising a plurality of data packets." In other words, Schneck is concerned with secure communications between computers, and not with monitoring of the security state of one computer by another. Element 106 in Figure 1 of Schneck is an entire computer system. Element 103 in Schneck is another computer system. There is no teaching in Figure 1, or anywhere in Schneck, that computer system 103 in Schneck monitors the security state system 103. Schneck instead discloses that computer system 106 receives encrypted information from computer 103, and uses portions of the encrypted information to decide on a security level for information exchange between the computer systems. Operation of Schneck's secure communications system is described in the following passages of Schneck, the first beginning on line 35 of column 4 and the second beginning on line 11 of column 6.

> The send host 103 includes a signature generator 116 which generates a signature block 119 from the data block 109 and the key 113 using a predetermined security algorithm which may be, for example, but not limited to, a security algorithm such as the Digital Signature Algorithm (DSA), the Rivest-Sharnir-Adleman (RSA) algorithm, or secret key authentication, which are generally known in the art.
>
> The send host 103 also includes an authentication header generator 123, which generates an authentication header 126. The authentication header 126 includes various data fields, such as, for example, an authentication sequence number, data frame size, frame type, security algorithm, verification type, minimum security level, target security level,

> and an actual security level. T*he receive host 106 employs these data fields to generate an actual security configuration to achieve authentication of a data stream communicated from the send host 103.* The actual security configuration is dynamic in that it may be changed by either the send host 103 or the receive host 106 during the course of data communication therebetween in response to user or application requirements, or changes in computer resource availability as will be discussed. (emphasis added)

> *Generally, the security levels as discussed herein refer to the percentage of verified data packets in the receive host 106. The security monitor 169 also determines the verification type as indicated by the first functional switch 153, as well as the specific security algorithm employed by both the delayed authentication verifier 156 and the percentage authentication verifier 163.*
>
> T*he security monitor 169 attempts to specify an actual verification type, actual security algorithm, and an actual security level according to the desired security configuration received from the send host 103. However, the receive host 106 may not have enough processor time or security operations per second (SOPS) to provide the desired security configuration due to the verification of other data streams which currently employ much of not all of the SOPS available in the receive host 106 at a given moment. Consequently, the security monitor 169 may force a change in the verification type, security algorithm, and/or the actual security level that differs from the desired security configuration received by the send host 103 in order to accommodate the data stream.* (emphasis added)

As the Examiner can hopefully appreciate, there is no teaching or suggestion that send host 103 monitors the security state of receive host 106. *Schneck is not concerned with, or directed to, the security state of any computer system.* Instead, Schneck is concerned with a negotiated, secure communication of data between two computer systems. It would seem that the Examiner noticed block 169, labeled "Security Monitor," in Figure 1 of Schneck and immediately assumed that this block was concerned with monitoring the security state of a computer system. As can be readily observed in the above-quoted passages, block 169 is concerned with configuring secure communications on the receive host according to information contained in data messages sent to the receive host by the send host.

Many different methods for secure communications are known. Many

involve using encryption keys to encrypt messages. That is extremely well known, and has been well known for many years. Schneck and Jones essentially provide different types of secure-communications methods. Secure communications is an element of the currently claimed invention. For example, in the final element of claim 1, claim 1 recites "a program, running on the computing device, that exchanges with the remote computer system, over the communications medium, messages encrypted using one or more encryption keys." However, claim 1 is directed to the monitoring of the security state of one computer system by another, as is stated repeatedly in both the preambles and the final elements of independent claims 1 and 9. Moreover, claim 1 expressly recites "a pair of data-storage media each containing a sequence of encryption keys." Neither Schneck nor Jones teaches, mentions, or even remotely suggests a pair of data-storage medium containing sequences of encryption keys, and neither Schneck nor Jones teaches, mentions, or even remotely suggests monitoring of the security state of one computer system by another.

In Applicant's representative's opinion, all of the claims remaining in the current application are clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,
Chris Hyser
Olympic Patent Works PLLC

Robert W. Bergstrom
Registration No. 39,906

Enclosures:
Postcard
Transmittal in duplicate

Olympic Patent Works PLLC
P.O. Box 4277
Seattle, WA 98194-0277
206.621.1933 telephone
206.621.5302 fax